

General and Technical Q and As

General Approved Questions

Q1. Why is the Order necessary?

Participants in these activities are receiving funding from various organizations and individuals.

The declaration and order aim to put a stop to funding the activities that contribute to the blockades.

Q2. What does the Order do to restrict the funding?

The Government is declaring a public order emergency to take the necessary steps to limit the funding of the activities that led to this current state of emergency.

This order requires all entities such as banks, credit unions, trust and loan companies, cryptocurrency exchanges and anyone providing financial services to take immediate steps to temporarily restrict access to funds to those involved in the blockades.

It requires banks and other financial services providers to cease, suspend or refuse, to provide services to any person or entity involved in the blockades, not to facilitate any transaction relating to funds or virtual currency, and not offer any financial service and providing any funding, including virtual currencies, to anyone involved in the blockades.

Q3. What will banks and other financial services providers be required to do under this order?

Banks and other financial service providers will have to take the following steps:

- * Review their records to identify if they have any business with persons involved in the blockades.
- * Freeze or suspend business relationships with anyone they identify involved in the blockades. This includes the suspension of access to deposit accounts, cryptocurrency wallets, lending products, and investments.

Q4. Banks have frozen accounts before. What is different?

[APG]

Financial service providers take action on a voluntary basis, which can vary from institution to institution. Currently, they can freeze accounts with a court order and can share information with law enforcement.

The order imposes a set of obligations to review their relationships with anyone involved in the blockades and report to the RCMP or CSIS.

A bank or other financial service provider will now be able to freeze or suspend an account without a court order. In doing so, they will be protected against civil liability for actions taken in good faith.

Government of Canada institutions will have a new broad authority to share information with banks and other financial service providers to ensure we all work together to put a stop to the funding of the blockades.

Q5. What safeguards will there be to protect Canadians?

These are temporary measures directed at restricting the funding of the blockades and will be in effect for 30 days.

Banks and financial service providers have to act in good faith.

The restriction on funds will cease to apply if affected individuals are no longer involved in the blockades.

Affected individuals will also have access to the courts.

Q6. Will this apply to entities regulated by provinces such as credit unions?

Yes, this order applies to all financial services providers, including those regulated under provincial law. This includes provincial credit unions and caisses populaires, provincial companies and securities dealers.

Q7. Does the Order cover cryptocurrencies?

Yes, this order is broad and covers assets and entities such as digital assets, crypto-currencies, payment processors and funding platforms. This order requires them to take action immediately.

Q8. Will the RCMP be able to share information with banks and other financial entities?

The order includes the ability for the RCMP and other provincial (including local police) and territorial law enforcement agencies, together with other institutions of the Government of

[APG]

Canada, to share information with banks and other financial services providers if they are satisfied that it will help with implementation of the order.

The information shared could include the names of persons and entities that are involved in the blockades. The RCMP and law enforcement agencies will continue to share information in accordance with their investigation processes.

[APG]

Additional Technical Questions

N.B. All questions below were not part of the Q&A approved by Isabelle.

Q9. What is the standard for banks to freeze and unfreeze access to the accounts of designated persons?

Banks and other federal or provincial deposit-taking institutions generally have procedures in place to identify suspicious transactions or accounts.

Upon the coming into force of the *Emergency Economic Measures Order*, they will need to identify among their clients, any individual or entity that is engaged, directly or indirectly, in an activity prohibited by the *Emergency Measures Regulations*.

The decision to freeze an account should be based on a reasonable suspicion that it is used to further such prohibited activities. Financial service providers are required to unfreeze accounts when the account holder stops participating in the illegal blockades.

Q10. Why must financial services providers share information about the property of designated persons with CSIS or the RCMP?

Information must be shared with CSIS or the RCMP for the purpose of assisting these organizations in conducting any investigations related to the unlawful activities noted in the declaration.

This is consistent with requirements set out in regulations to support international economic sanctions against persons engaged in prohibited activities.

Q11. What evidence will demonstrate that the actions required by the Order are effective?

A significant amount of money is being sent through platforms such as crowdfunding sites and into accounts to support the blockades. These measures are designed to limit that flow and prevent further financial support.

A second strategic objective of the temporary measures is to prevent Canada's financial system from being used to finance the illegal blockades or any other activity prohibited by the *Emergency Measures Regulations*.

[APG]

Q12. Does the Order apply to anyone who donates to blockade participants?

The measures taken under the proclamation of the public order emergency specify the blockades as part of the emergency and prohibit people from providing property for the purpose of benefitting any person who is facilitating or participating in a blockade.

[Responsive] If asked if a person who donates to the protestor will have their account frozen?

Anyone or any entity that participates directly or indirectly in a prohibited activity is exposing themselves to financial risks and should stop.

Q13. Aren't you exposing others to risk if you suspend protestors' vehicle insurance?

When an individual stops participating in an illegal activity and leaves the places where they are occurring, we expect the measures to not apply.

Anyone participating in these activities risks the suspension of their accounts and vehicle insurance.

[Responsive] If asked about a protestor having an accident.

We expect insurance companies to ensure that third parties can continue to benefit from an insurance payout.

Q14. Will individuals be able to continue their financial relationship after the order is lifted?

For the most part financial institutions can decide who they do business with and may decide to continue or cease to offer any financial services.

In the banking sector, the access to banking services regulations require banks to open bank account under certain conditions. The Financial Consumer Agency of Canada is responsible for the application of these regulations.

[APG]

Crowdfunding and Payment Service Provider Registration and Reporting

Key Messages:

- Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), financial institutions and other entities are subject to due diligence and reporting requirements aimed at identifying individuals involved in illicit finance activities.
- Recent activities have highlighted the fact that crowdfunding platforms and some payment service providers are not currently subject to the obligations under the PCMLTFA and may be used to finance illegal activities.
- The measures contained in the Order will ensure that crowdfunding platforms and payment service providers that hold funds of those involved in the blockades are **immediately obligated to:**
 - **Register with FINTRAC;**
 - **Report suspicious transactions to FINTRAC; and,**
 - **Report large value transactions (\$10,000 or more) to FINTRAC.**
- These new requirements will increase the quality/quantity of intelligence received by FINTRAC and the ability of law enforcement agencies to identify and take action against those involved in illicit finance activities.

Q: What would these changes mean in practice?

A: Extending anti-money laundering and anti-terrorist financing requirements to crowdfunding platforms and payment service providers will not modify the powers of the Minister of Finance or Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). It will ensure that where these entities hold funds of those involved in the blockades they are obligated to:

- Register with FINTRAC;
- Report any suspicious transaction to FINTRAC.
- Report large value transactions (\$10,000 or more) to FINTRAC.

This will help mitigate risks that these platforms receive illicit funds, increase the quality/quantity of intelligence received by FINTRAC, and make more information available to support investigations by law enforcement.

Q: What are the limitations of these changes?

A: FINTRAC does not have the authority to track or monitor financial transactions in real time, nor does it freeze assets or investigate potential criminal activities. The RCMP and other policing bodies would remain responsible for investigating crime.

[APG]

While foreign crowdfunding platforms and the payment service providers they use would be captured, enforcement of regulatory requirements could be more limited.

The obligations would not be applied retroactively.

Q: How quickly will these new requirements come online?

A: Under the terms of the Order, all persons and entities that are engaged in the business of providing a platform to raise funds or virtual currency through donations, or providing a payment function will **immediately** have to register with FINTRAC, and **immediately** begin reporting suspicious transactions and large value transactions to FINTRAC, if they hold funds of those involved in the blockades.

Q: Do these changes cover the use of cryptocurrencies?

A: Yes. Anti-money laundering and anti-terrorist financing requirements under the PCMLTFA already apply to businesses dealing in virtual currencies (i.e. cryptocurrencies), including requirements to register with FINTRAC, conduct customer due diligence, keep records, and report large value and suspicious transactions.

All persons and businesses regulated under the PCMLTFA are also required to report the receipt of large virtual currency transactions to FINTRAC. Under the order, suspicious reporting and large value reporting requirements have been extended to crowdfunding platforms and payment service providers.

Q: Can cryptocurrency be used to evade this order?

A: Businesses that “deal” in virtual currency (i.e. cryptocurrencies) are already regulated under the PCMLTFA, and have obligations to register with FINTRAC, verify client identity, keep records, and report transactions.

“Dealing in virtual currency” refers to the exchange or transfer of virtual currency. This includes the purchase of virtual currency using fiat currency (e.g. Canadian or US dollars) or another type of virtual currency, as well as sending virtual currency from one virtual currency business to another. As soon as the virtual currency is converted into fiat currency (e.g. Canadian dollars) or another virtual currency, or transferred to a wallet hosted by a regulated business, regulatory obligations under the PCMLTFA would be triggered.

However, these controls would not apply to peer-to-peer transactions where no regulated business is involved. This would include the transfer of virtual currency from one un-hosted wallet (i.e. self-hosted or non-custodial wallet) to another.

Q: Do any other jurisdictions regulate crowdfunding for anti-money laundering and anti-terrorist financing? What about payments service providers?

A: The Financial Action Task Force, the international standards setting body for anti-money laundering and anti-terrorist financing, has recognized the risks of crowdfunding being used by

[APG]

illicit actors. The European Council is expected to provide a report in November 2023 to advise on the necessity of regulating crowdfunding. To our knowledge, Canada may be the first country to regulate crowdfunding for anti-money laundering and anti-terrorist financing purposes.

Other jurisdictions such as Australia, and European Union member states regulate payment service providers for anti-money laundering and anti-terrorist financing purposes.

Q: What does this mean for a payment service provider already covered under the PCMLTFA?

A: Payment services providers in Canada that engage in certain activities are considered “money services businesses” and are already regulated under the PCMLTFA. This includes reporting requirements to FINTRAC, registration with and supervision by FINTRAC. As the order replicates certain existing requirements of the PCMLTFA, payment services providers who are already regulated would not have any new obligations.

Q: Does this order apply to foreign crowdfunding platforms and payment service providers?

A: Yes, this order applies to foreign crowdfunding platforms and payment service providers. The measures contained in the Order will ensure that foreign, as well as domestic, entities are immediately obligated to:

- Register with FINTRAC;
- Report any suspicious transaction to FINTRAC; and,
- Report large value transactions (\$10,000 or more) to FINTRAC.

Q: Are all crowdfunding platforms and payment services providers covered by this order, or just those holding funds of those involved in the blockades?

A: A number of payment service providers are already subject to the requirements of the PCMLTFA. The order refers to crowdfunding platforms and payment services providers that hold funds of those involved in the blockades (designated persons) in order to respect the scope of these emergency measures. The government will bring forward regulations to implement these requirements on a permanent basis with respect to all crowdfunding platforms and payment services providers.

Q: What will be the burden of these measures?

A: We estimate 1,500-2,000 payment service providers would be subject to the new *Retail Payments Activities Act*, and the order uses a similar definition. About 80% of these entities are already subject to the PCMLTFA requirements as money services businesses.

Many crowdfunding platforms have terms of reference and internal teams dedicated to mitigate money laundering and terrorist financing risks that these platforms pose. As with all sectors, the government will develop requirements that mitigate anti-money laundering and anti-terrorist

[APG]

financing risks, while minimizing administrative burden, and respecting privacy laws and the *Charter of Rights and Freedoms*.

Annex – Background Information

CROWDFUNDING

- **Crowdfunding** is the practice of funding a project or venture by raising financial contributions from a number of people, typically through online platforms, in order to carry out a project, investment or other endeavor requiring funds. Crowdfunding campaigns are often completed in conjunction with a dedicated crowdfunding platform or by initiating informal appeals through social media. A crowdfunding platform, also called a funding portal, posts crowdfunding projects on its website. Estimates of the sector vary. Globally, the crowdfunding industry is estimated to be worth US\$10.2 billion in 2018 and is expected to reach US\$28.8 billion by the end of 2025.
- Unlike traditional fundraising methods (e.g. loans from financial institutions), crowdfunding allows individuals or groups to appeal for funds directly from members of the public. Crowdfunding platforms enable those connected online or through social media, who may be geographically dispersed, to pool resources towards common goals and projects that require financing.

PAYMENT SERVICE PROVIDERS

- **Payment service providers (PSPs)** include a variety of entities that perform electronic payment functions, such as payment processors, digital wallets, currency transfer services, and other payment technology companies that offer any of the following services:
 - providing and maintaining a payment account;
 - holding funds until the end user withdraws or transfers them;
 - initiating an electronic funds transfer as requested by an end user;
 - authorizing or transmitting instructions about an electronic funds transfer;
 - and
 - clearing or settling electronic funds transfers

CROWDFUNDING AND PSPs

- Many of the crowdfunding platforms that currently exist use third party **PSPs** to enable the completion of payments. This means that the information related to the transaction as well as the movement of money itself, is fragmented along a number of different entities, but would most likely be held with the PSP, rather than the crowdfunding platform lending its services to an individual or entity engaged in fundraising.

CROWDFUNDING AND FINTRAC DATA

- Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, FINTRAC does not have the authority to track or monitor financial transactions in real time.

[APG]

- The Centre receives approximately 30 million financial transaction reports a year from businesses subject to the Act, including reports on international electronic funds transfers (EFTs) totaling \$10,000 or more within a 24 hour period; large virtual currency transactions totaling \$10,000 or more within a 24 hour period; and suspicious transactions, which have no monetary threshold for reporting.

[APG]

[APG]